

**atmosphere'22**  
MAKING CONNECTIONS, ANYWHERE



# Enhance SD-WAN Security With Zero Trust and SASE

**aruba**  
a Hewlett Packard  
Enterprise company

# Agenda

- Aruba at the Edge
- Traffic Directionality
- Zero Trust and SASE in Practice

# Aruba Secure Edge Portfolio

## Data Center and Branch App & Services



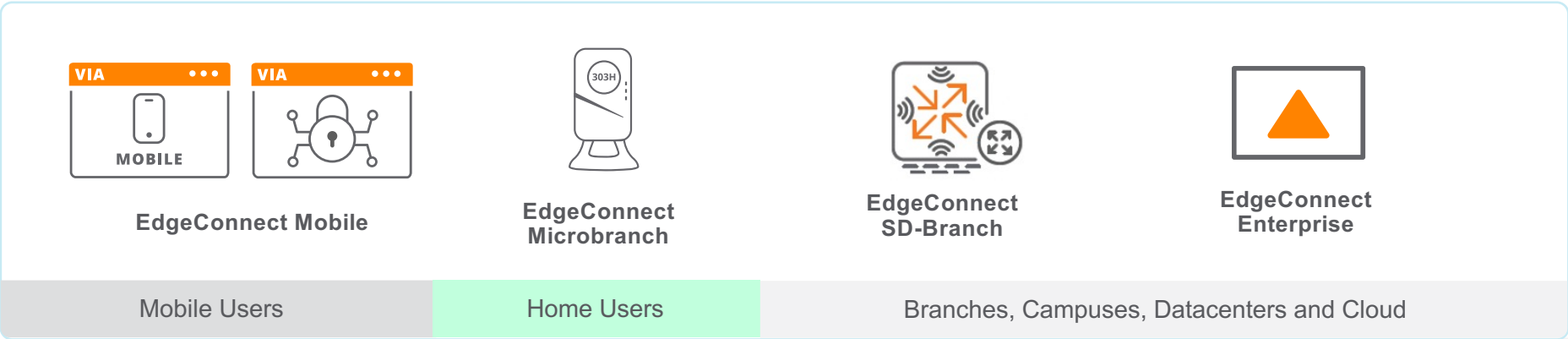
## Cloud Hosted Apps and Services (IaaS)



## SaaS, Cloud Based Services



## Secure, Optimized, Protected SD-WAN Fabric



# Aruba Secure Edge Portfolio



## ZERO TRUST

- Aruba ClearPass
- Zscaler Zero Trust Access
- Fine-Grained Segmentation
- Rich identity-based context – device type, user role, and security posture

## SD-WAN

- Aruba UTM (IDPS) with EdgeConnect
- Next Gen Firewall
- E2E Network Segmentation
- Secure internet breakout
- SD-WAN, Routing, WAN Op, and Network visibility and control

## CLOUD SECURITY

- Best-of-Breed cloud security approach
- Service Orchestration to Zscaler
- Local Internet Breakout
- Cyber Threat Protection
- Data Protection (DLP, CASB)
- Internet Workload



## SECURE ACCESS SERVICE EDGE (SASE)

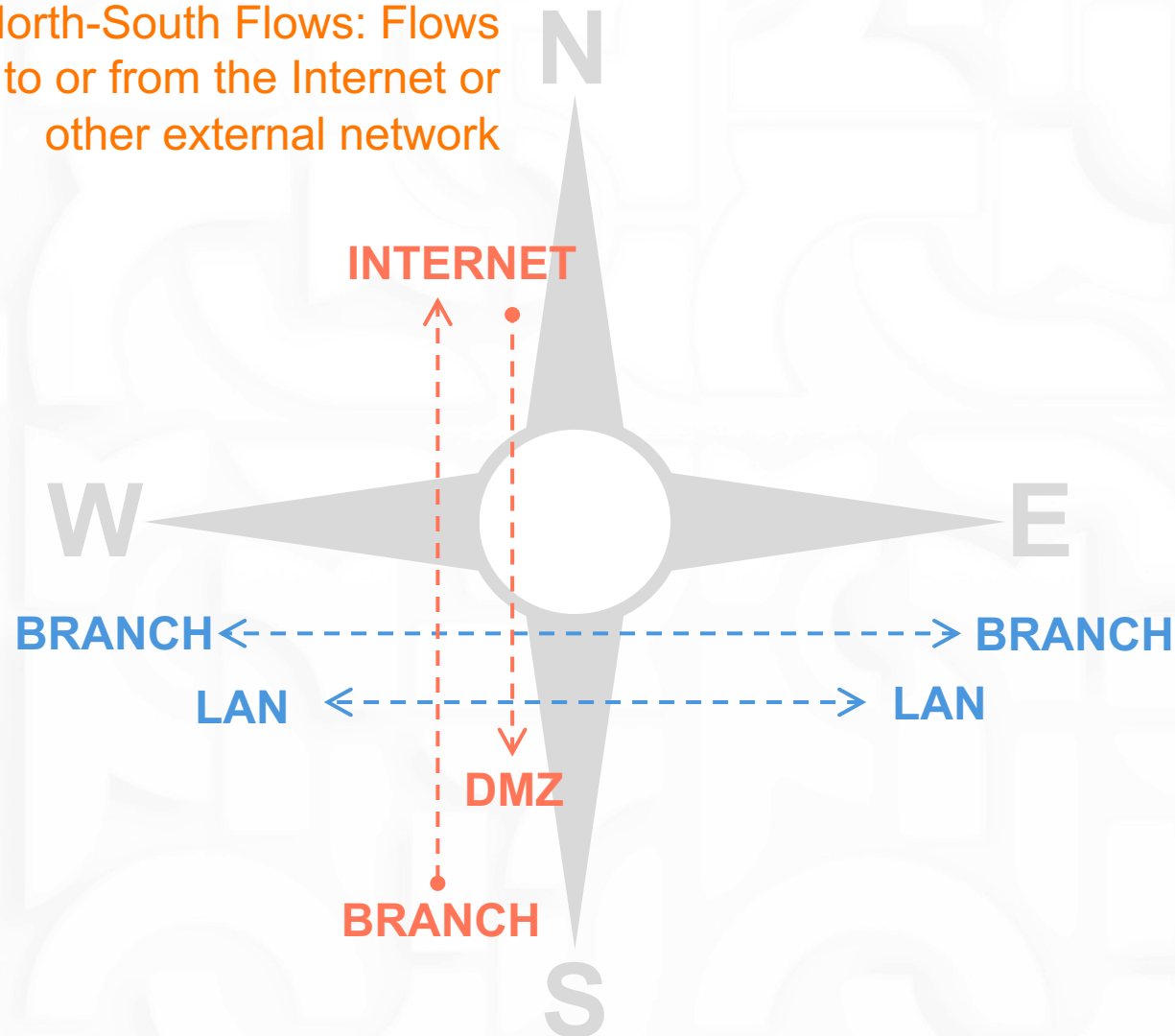


# Traffic Directionality

# East-West: Flows within the Fabric and within the Branch or Campus

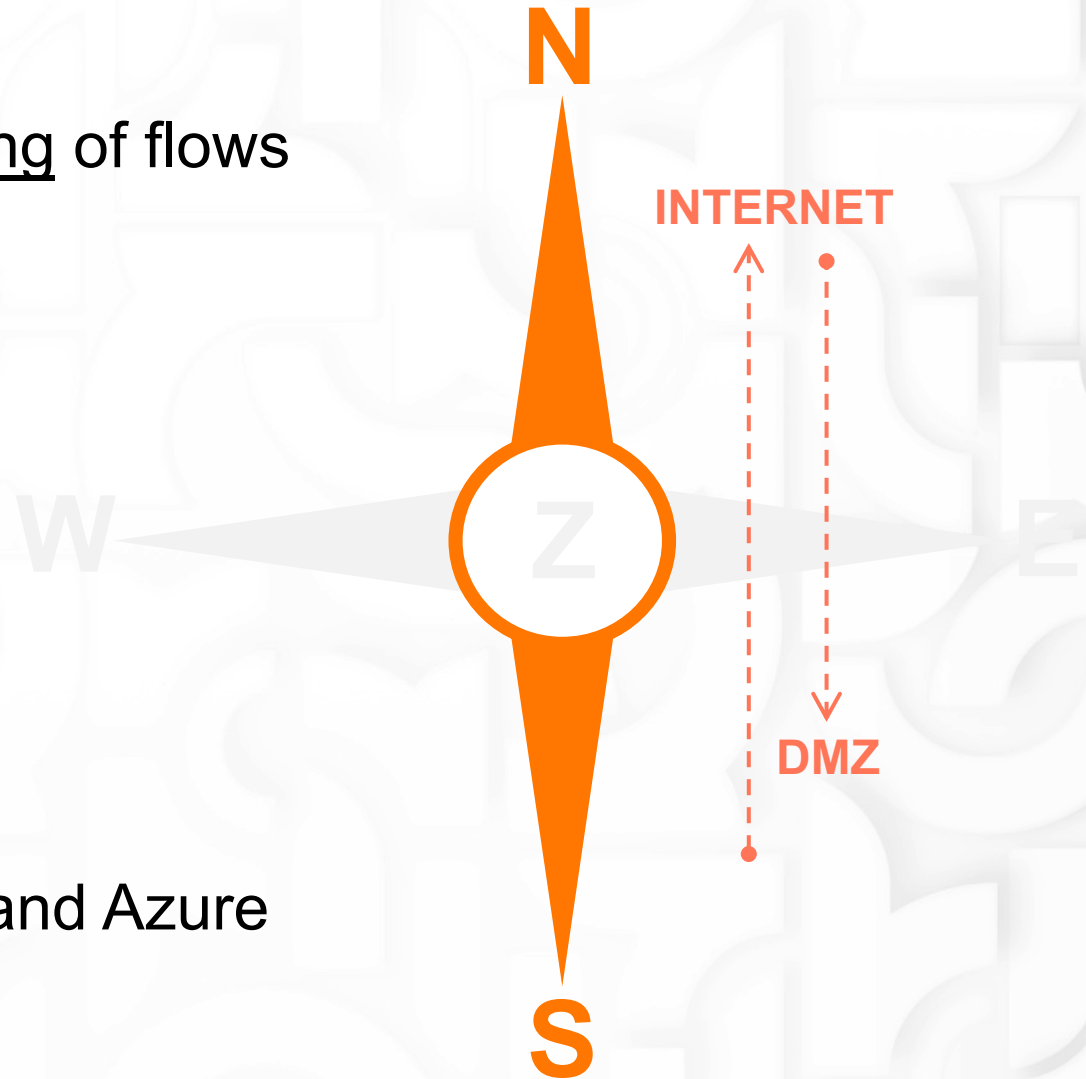
North-South Flows: Flows to or from the Internet or other external network

East-West: Flows within the Branch or Campus and **within the Fabric**



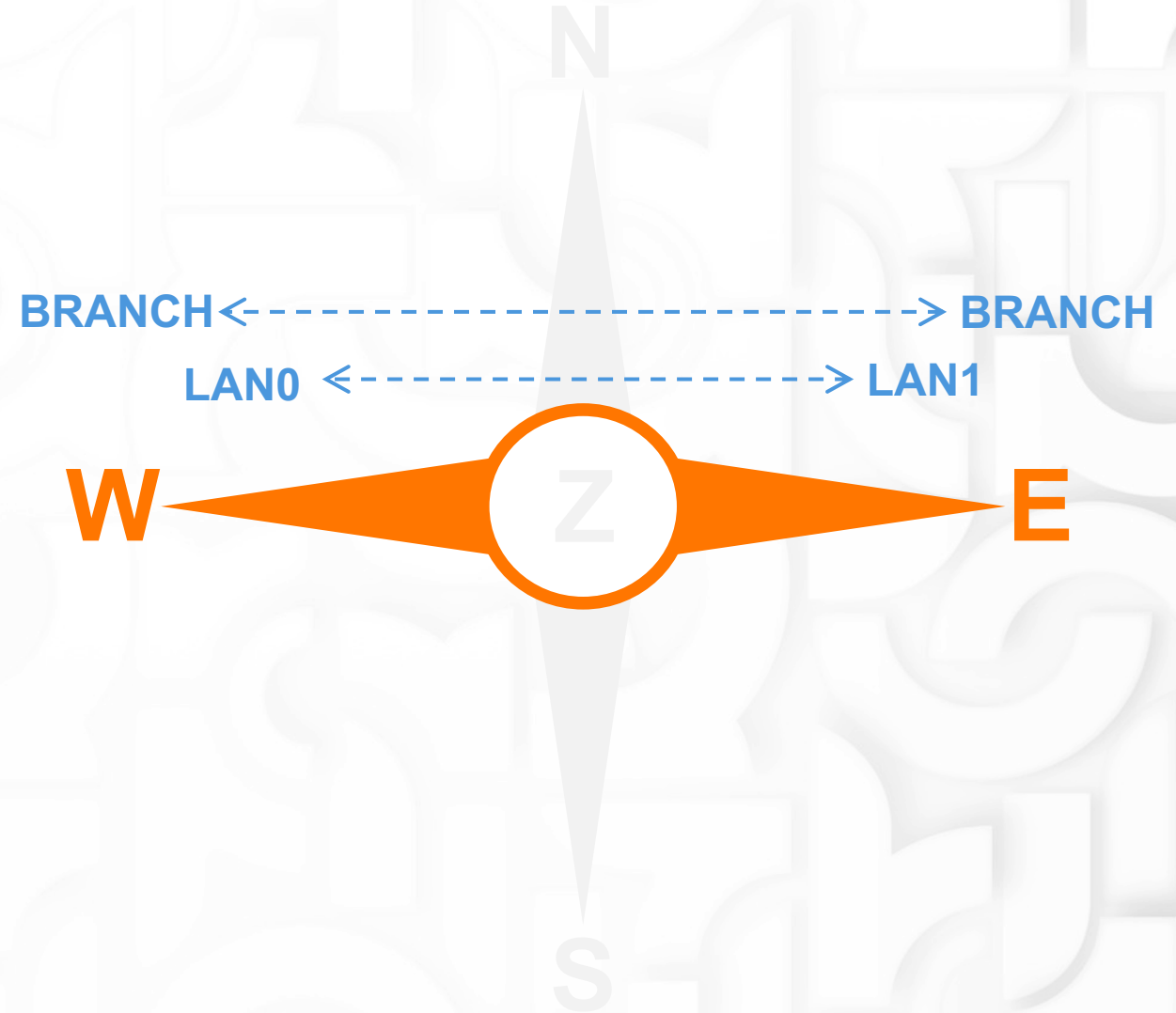
# Security Architecture for North-South Traffic

- First-packet inspection provides steering of flows to the correct north-bound service
- DoS Protection
- DMZ and Port Forwarding Support
- Intrusion Detection and Prevention
- Automation for Zscaler, Netskope, etc.
- Automation for AWS Transit Gateway and Azure vWAN (IPSEC+BGP)



# Security Architecture for East-West Traffic

- Zone and/or Identity-based firewall controls traffic between users and sites
- Intrusion Detection and Prevention can be applied to any east-west flows, selectable by application, zone, etc
- DoS protection for lateral attacks
- Routing Segmentation for Layer 3 isolation of users, groups, device types, etc.
- Dynamic Segmentation



# Securing the Edge

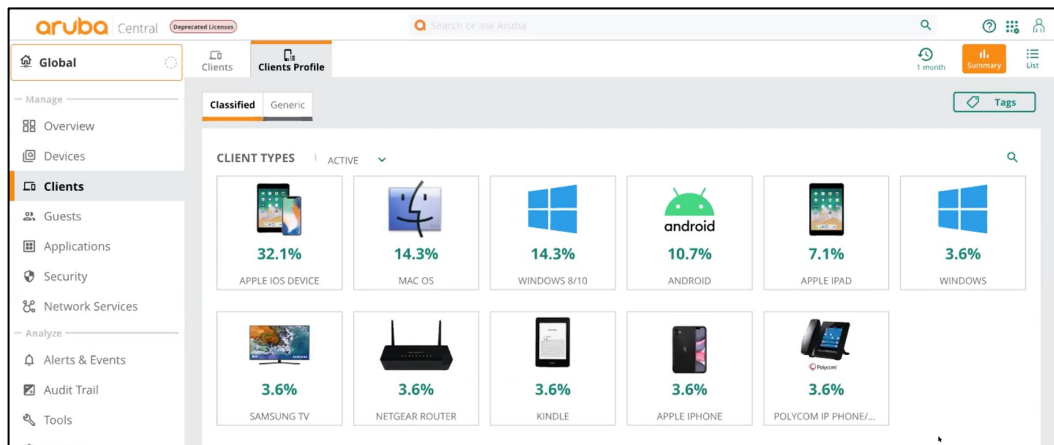






## Device Profiling integrated in Central

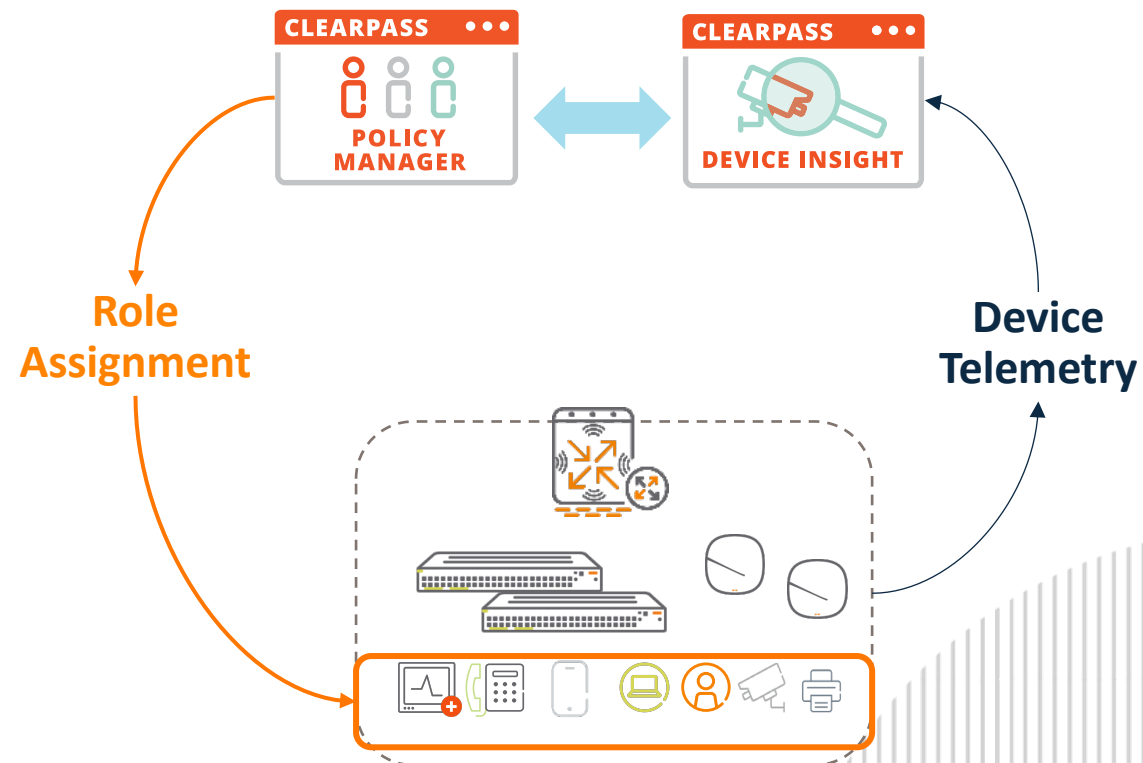
- AI/ML driven device profiling, based on static attributes like DHCP fingerprint or MAC OUI (APs)
- Also based on dynamic traffic flows learnt as part of the telemetry sent to Aruba Central.

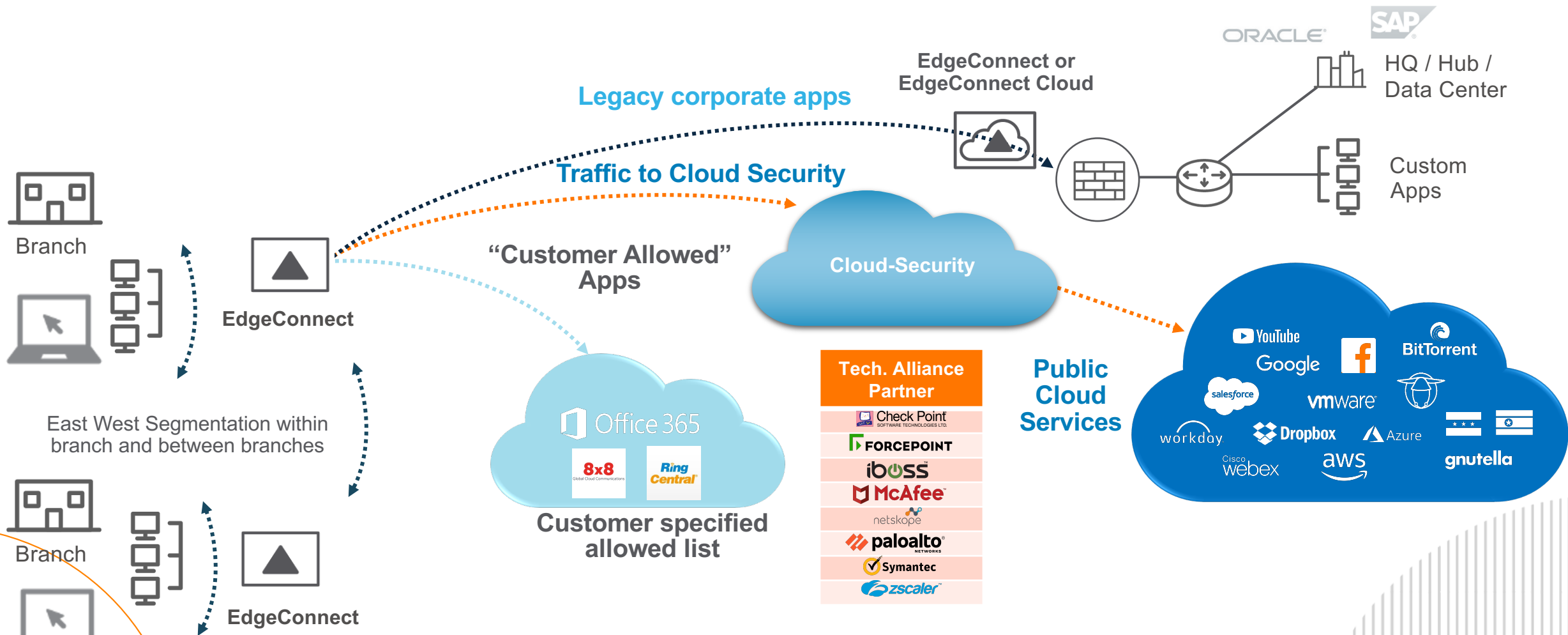


## Application Identification

- Identify application on first packet to ensure classification is correct at start of flow

## Device information seamlessly shared with ClearPass to assign user roles



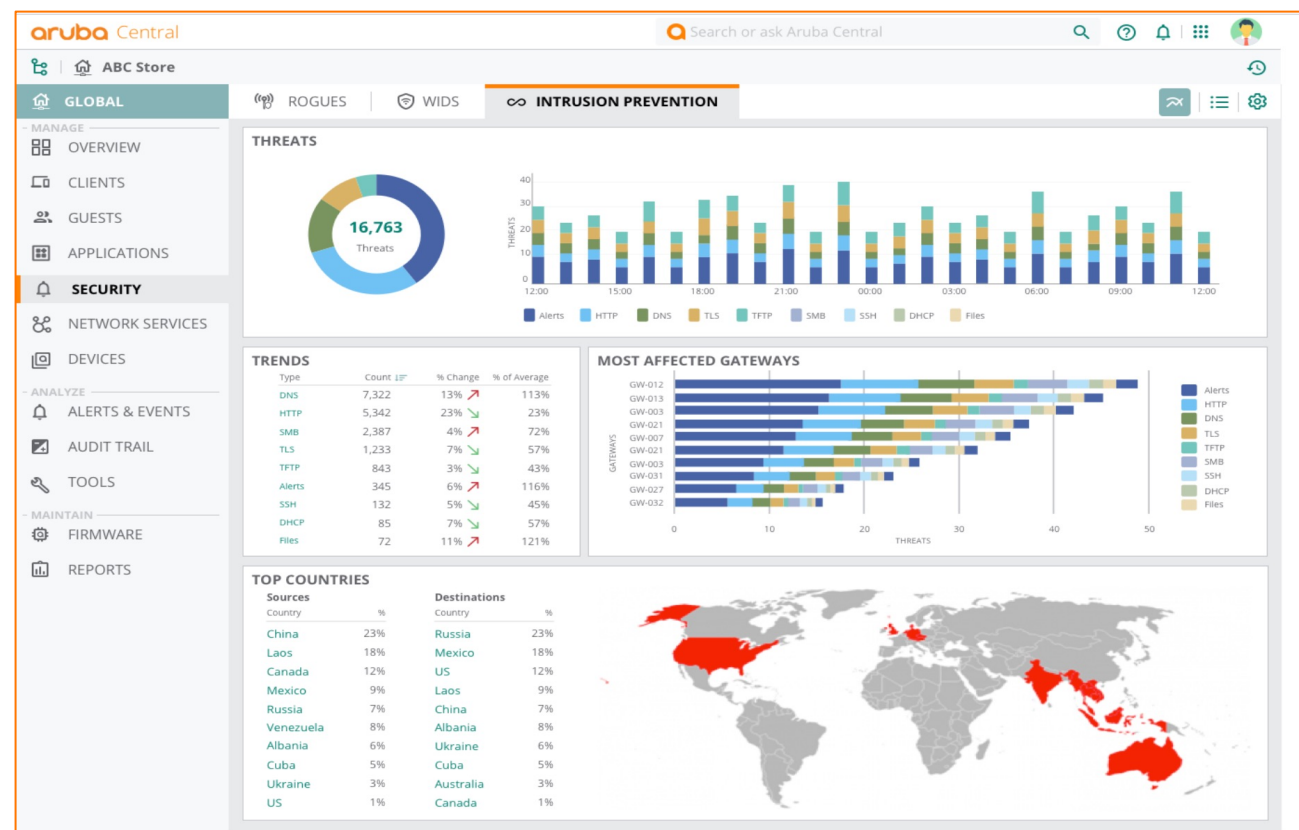




## Integrated IDS/IPS

- Real-time information via dashboard/alerting framework
- Integration with SIEM providers
  - Native integration with Splunk
  - Webhooks to customize integration with any other SIEM
- Ruleset driven
  - Pattern based

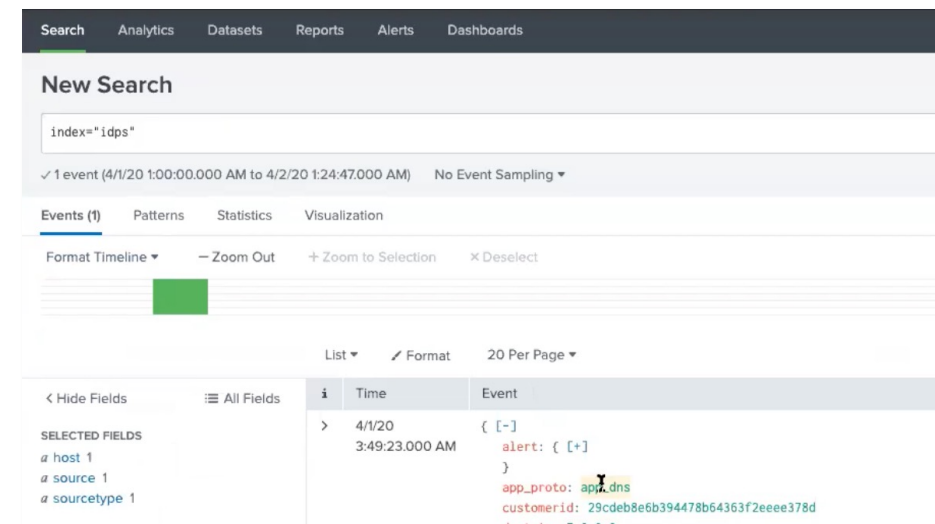
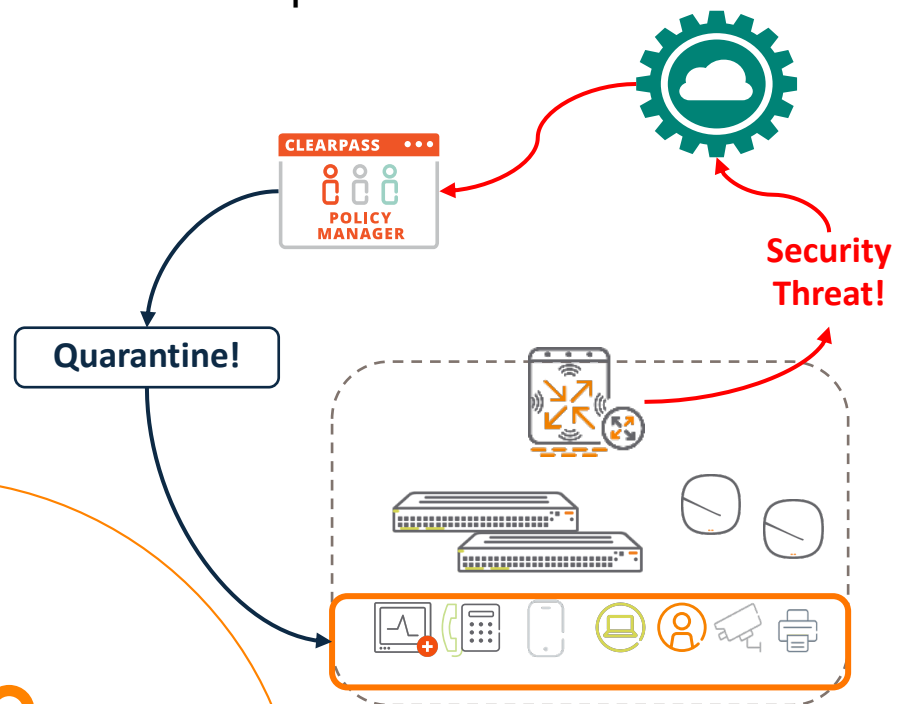
## Built-In Security Dashboard





## Threat response

- Alerting
- SIEM Integration
- Close loop with SIEM / ClearPass Integration



servicenow Service Management

Filter navigator

Incidents New Search Updated ▾ Search

1 to 20 of 79

	Number	Opened	Short description	Priority	State	Category	Assignment group	Assigned to	Updated
	INC0011200	2021-06-14 11:52:29	Gateway Control CONNECTION Down	1 - Critical	New	Inquiry / Help	(empty)	(empty)	2021-06-14 12:44:58
	INC0011204	2021-06-14 12:40:03	DPS_COMPLIANCE_ALERT	3 - Moderate	New	Inquiry / Help	(empty)	(empty)	2021-06-14 12:40:03
	INC0011203	2021-06-14 12:40:03	DPS_COMPLIANCE_ALERT	3 - Moderate	New	Inquiry / Help	(empty)	(empty)	2021-06-14 12:40:03
	INC0011199	2021-06-14 11:50:01	GW_IDS_IPS_ALERT_THREAT_OVER_A_PERIOD	3 - Moderate	New	Inquiry / Help	(empty)	(empty)	2021-06-14 12:00:03
	INC0011201	2021-06-14 12:00:03	DPS_COMPLIANCE_ALERT	3 - Moderate	New	Inquiry / Help	(empty)	(empty)	2021-06-14 12:00:03
	INC0011202	2021-06-14 12:00:03	DPS_COMPLIANCE_ALERT	3 - Moderate	New	Inquiry / Help	(empty)	(empty)	2021-06-14 12:00:03
	INC0010957	2021-03-15 20:04:15	AP disconnected	1 - Critical	New	Inquiry / Help	(empty)	(empty)	2021-03-15 10:58:15

Self-Service

Benchmarks

Dashboard

Administration

- Setup
- Category

Business Calendar

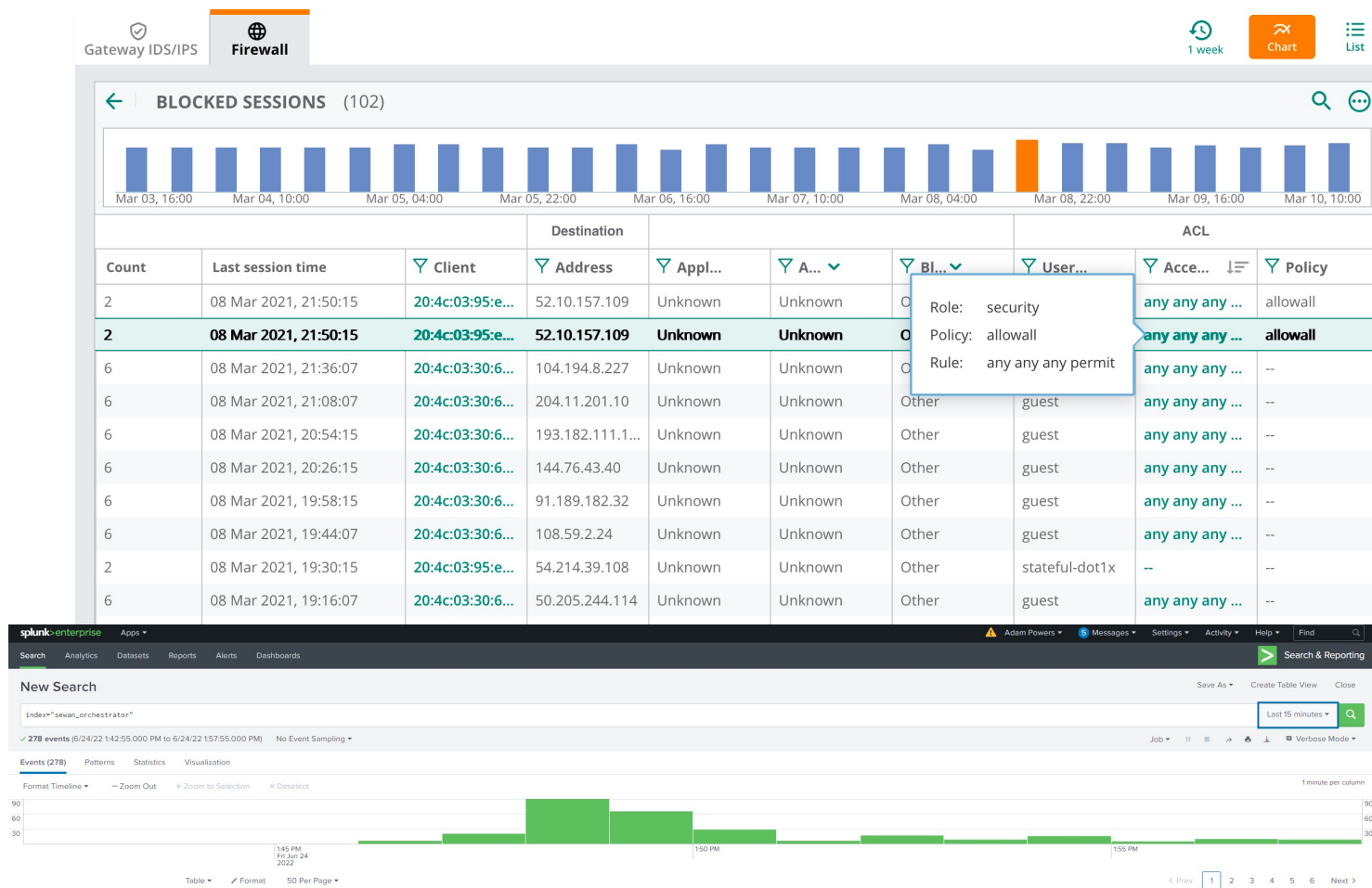
Guided Setup

Guided Tour Designer



## Security Logging

- Blocked session
- IPFIX
- Gateway Firewall
- Streaming API
- Splunk App for threat analysis
- ServiceNow alarm integration plug-in





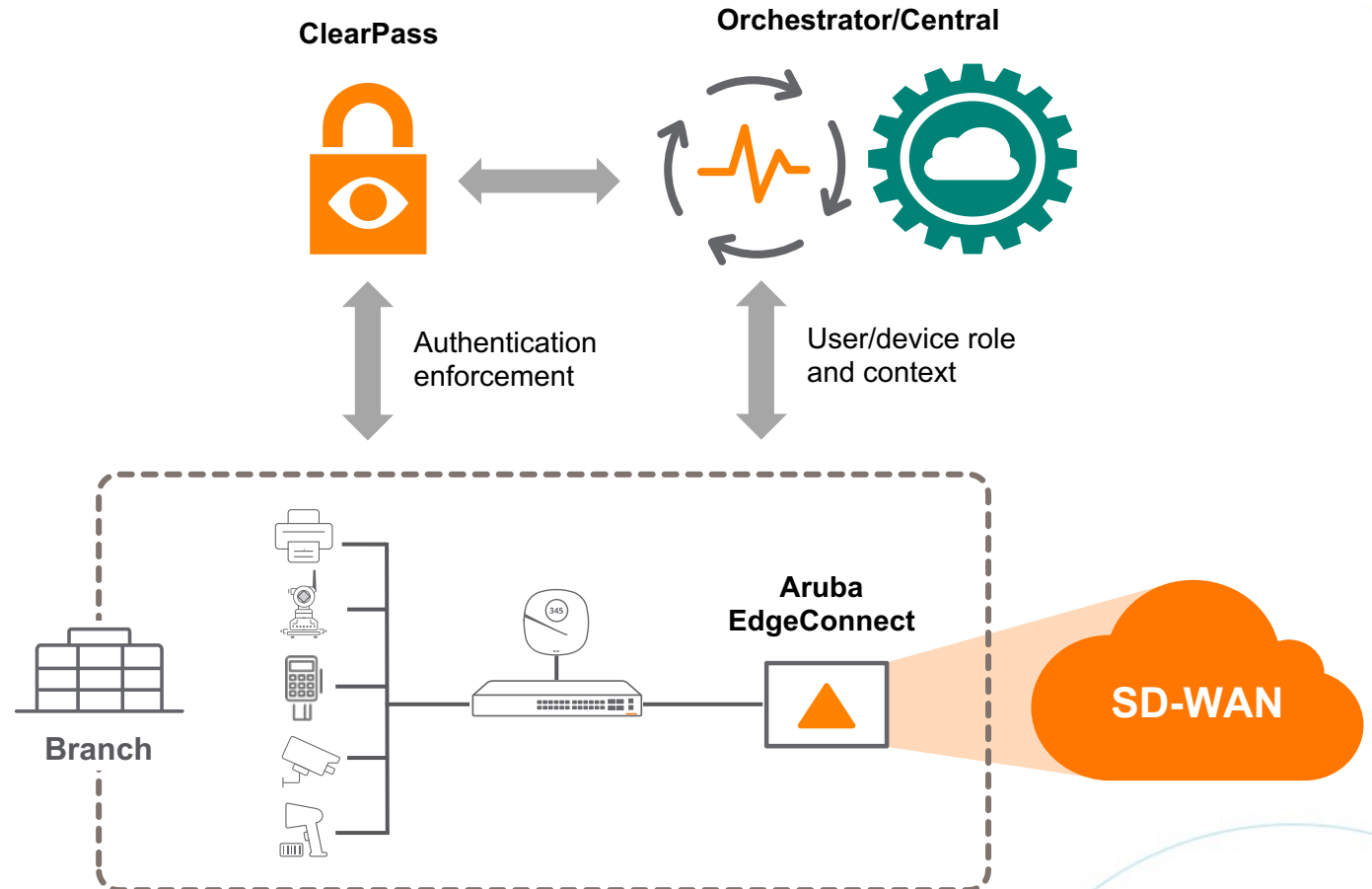
# Zero Trust and SASE in Practice

# Zero Trust with Aruba

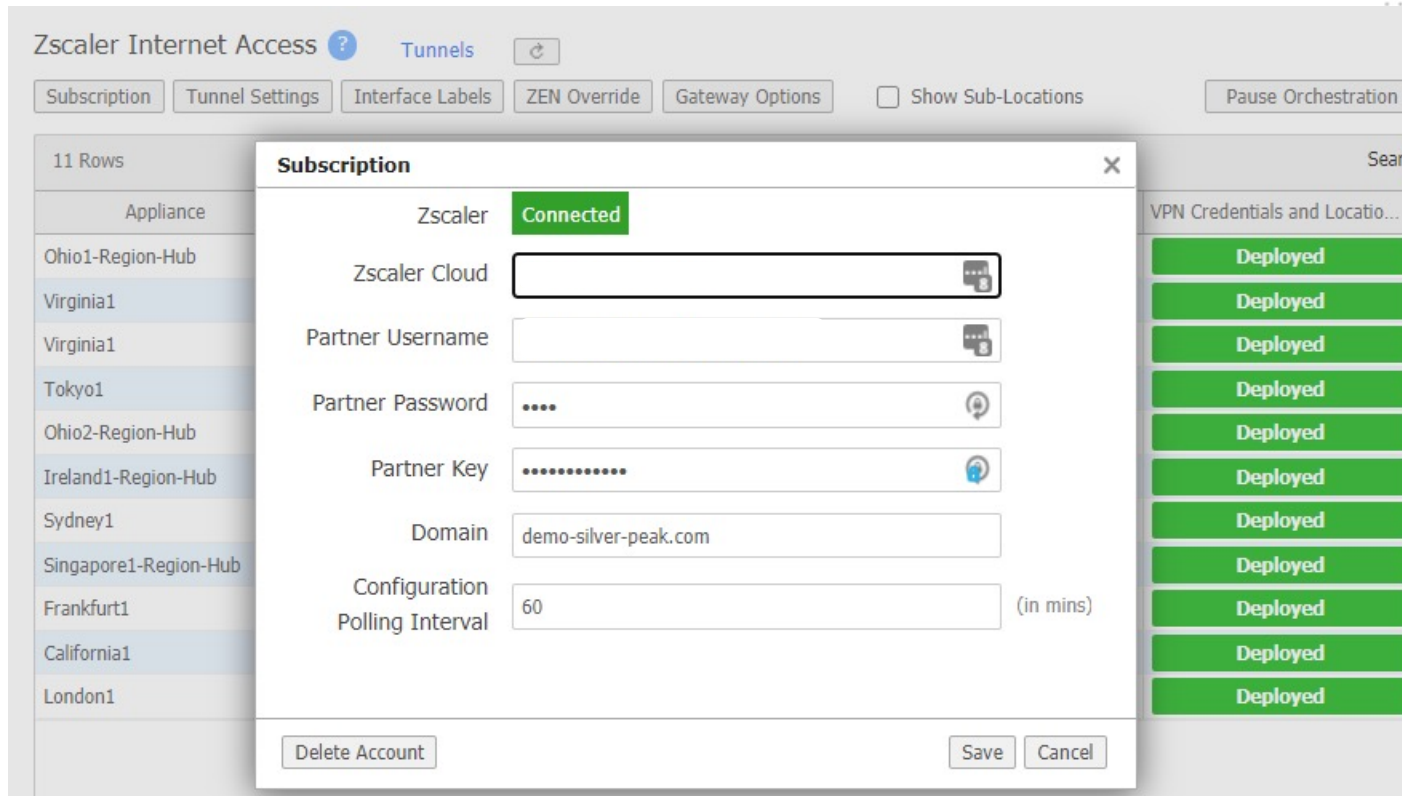
Visibility, control, response

**Single platform automates enterprise-wide context-aware, role-based policy**

- **Visibility and automation:**
  - Built-in discovery, profiling and dashboards
  - Multi-vendor wired, wireless and VPN
- **Control:**
  - Access control of users/devices
- **Response:**
  - Adaptive response and dynamic segmentation
- **360 Security integrations:**
  - Ecosystem of 150+ security partners
- **Leverage multiple identity stores:**
  - Support for AD, LDAP, SQL, Internal dB, BYOD, third party integration



# SASE Service Orchestration with Aruba



- Fully automated orchestration to Zscaler
  - Automatic Geolocation
  - Automatic HA
  - Performance Based Steering
- Automated tunnel orchestration to Check Point, McAfee, Netskope, Prisma and Symantec
- Auto-configuration of IPSLA monitoring rules
- Simple drag-and-drop policy orchestration in the overlays

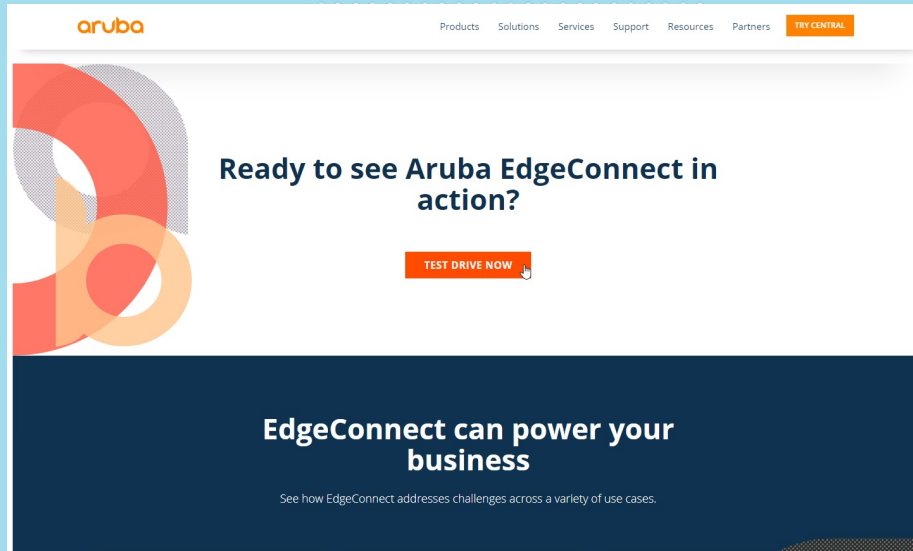


# Key Points

- Zero-Trust Architecture requires a new mindset and network that supports it
- Understand types of segmentation and use them wisely
- On-Premise security is very much “still a thing”
- Delegate advanced north-south security through policy orchestration
- Never forget the reason the network exists: **CONNECTIVITY**

# TAKE IT FOR A TEST DRIVE

[arubanetworks.com/test-drive-SD-WAN](https://arubanetworks.com/test-drive-SD-WAN)



aruba

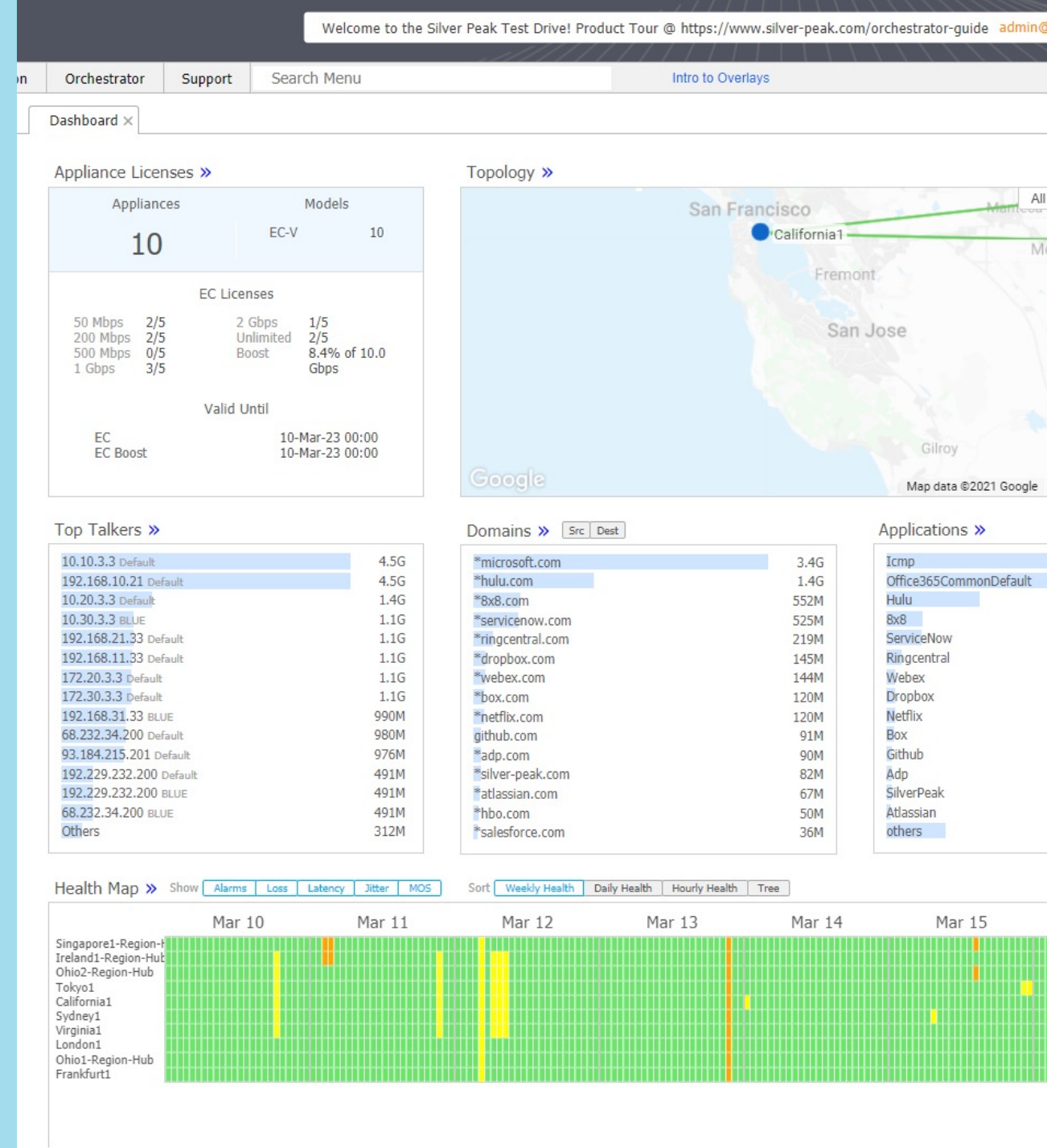
Products Solutions Services Support Resources Partners TRY CENTRAL

Ready to see Aruba EdgeConnect in action?

TEST DRIVE NOW

EdgeConnect can power your business

See how EdgeConnect addresses challenges across a variety of use cases.



Welcome to the Silver Peak Test Drive! Product Tour @ <https://www.silver-peak.com/orchestrator-guide> admin@

Orchestrator Support Search Menu Intro to Overlays

Dashboard x

### Appliance Licenses >>

Appliances		Models	
10		EC-V	10

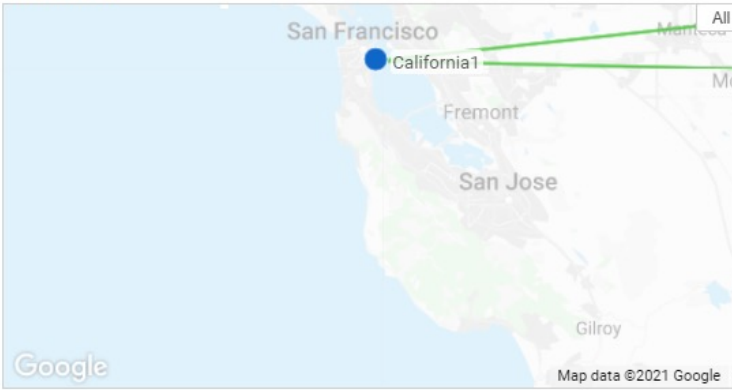
#### EC Licenses

50 Mbps	2/5	2 Gbps	1/5
200 Mbps	2/5	Unlimited	2/5
500 Mbps	0/5	Boost	8.4% of 10.0 Gbps
1 Gbps	3/5		

#### Valid Until

EC	10-Mar-23 00:00
EC Boost	10-Mar-23 00:00

### Topology >>



### Top Talkers >>

IP Address	Default	Size
10.10.3.3	Default	4.5G
192.168.10.21	Default	4.5G
10.20.3.3	Default	1.4G
10.30.3.3	BLUE	1.1G
192.168.21.33	Default	1.1G
192.168.11.33	Default	1.1G
172.20.3.3	Default	1.1G
172.30.3.3	Default	1.1G
192.168.31.33	BLUE	990M
68.232.34.200	Default	980M
93.184.215.201	Default	976M
192.229.232.200	Default	491M
192.229.232.200	BLUE	491M
68.232.34.200	BLUE	491M
Others		312M

### Domains >>

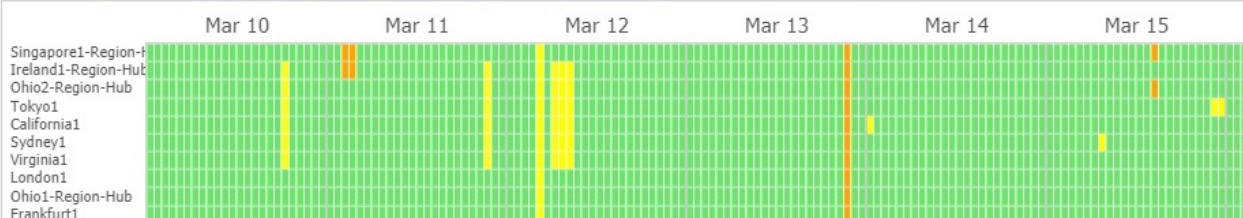
Domain	Size
*microsoft.com	3.4G
*hulu.com	1.4G
*8x8.com	552M
*servicenow.com	525M
*ringcentral.com	219M
*dropbox.com	145M
*webex.com	144M
*box.com	120M
*netflix.com	120M
github.com	91M
*adp.com	90M
*silver-peak.com	82M
*atlassian.com	67M
*hbo.com	50M
*salesforce.com	36M

### Applications >>

Icmp
Office365CommonDefault
Hulu
8x8
ServiceNow
Ringcentral
Webex
Dropbox
Netflix
Box
Github
Adp
SilverPeak
Atlassian
others

### Health Map >>

Show Alarms Loss Latency Jitter MOS Sort Weekly Health Daily Health Hourly Health Tree



Mar 10 Mar 11 Mar 12 Mar 13 Mar 14 Mar 15

Singapore1-Region-H  
Ireland1-Region-Hub  
Ohio2-Region-Hub  
Tokyo1  
California1  
Sydney1  
Virginia1  
London1  
Ohio1-Region-Hub  
Frankfurt1



# atmosphere'22

MAKING CONNECTIONS, ANYWHERE









# Thank you

<name@hpe.com>

Date 2022

**aruba**  
a Hewlett Packard  
Enterprise company

# Security Partner Ecosystem

Tech. Alliance Partner	Cloud Service	Level of Support
 <b>Check Point</b> SOFTWARE TECHNOLOGIES LTD.	CloudGuard Connect	Automated
 <b>FORCEPOINT</b>	Cloud security	Integrated
 <b>iboss</b> <sup>TM</sup>	Cloud security	Integrated
 <b>McAfee</b> <sup>TM</sup>	Unified Cloud Edge	Integrated
 <b>netskope</b>	SWG	Integrated
 <b>paloalto</b> <sup>®</sup> NETWORKS	Prisma Access	Integrated
 <b>Symantec</b>	Web Security Service	Integrated
 <b>zscaler</b> <sup>TM</sup>	Zscaler Internet Access	Automated

# Branch Security Across Fabric



App-user aware firewall



Deep packet inspection



Endpoint Profiling



Intrusion detection & prevention system



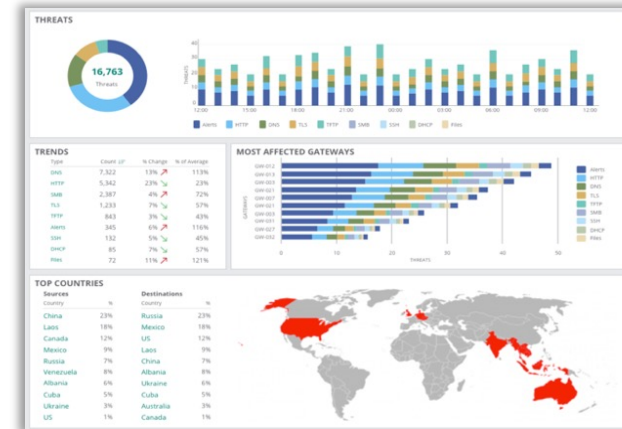
Web content & URL filtering



Zero Trust – Dynamic Segmentation



VRF – Advanced Segmentation



## Threat visibility

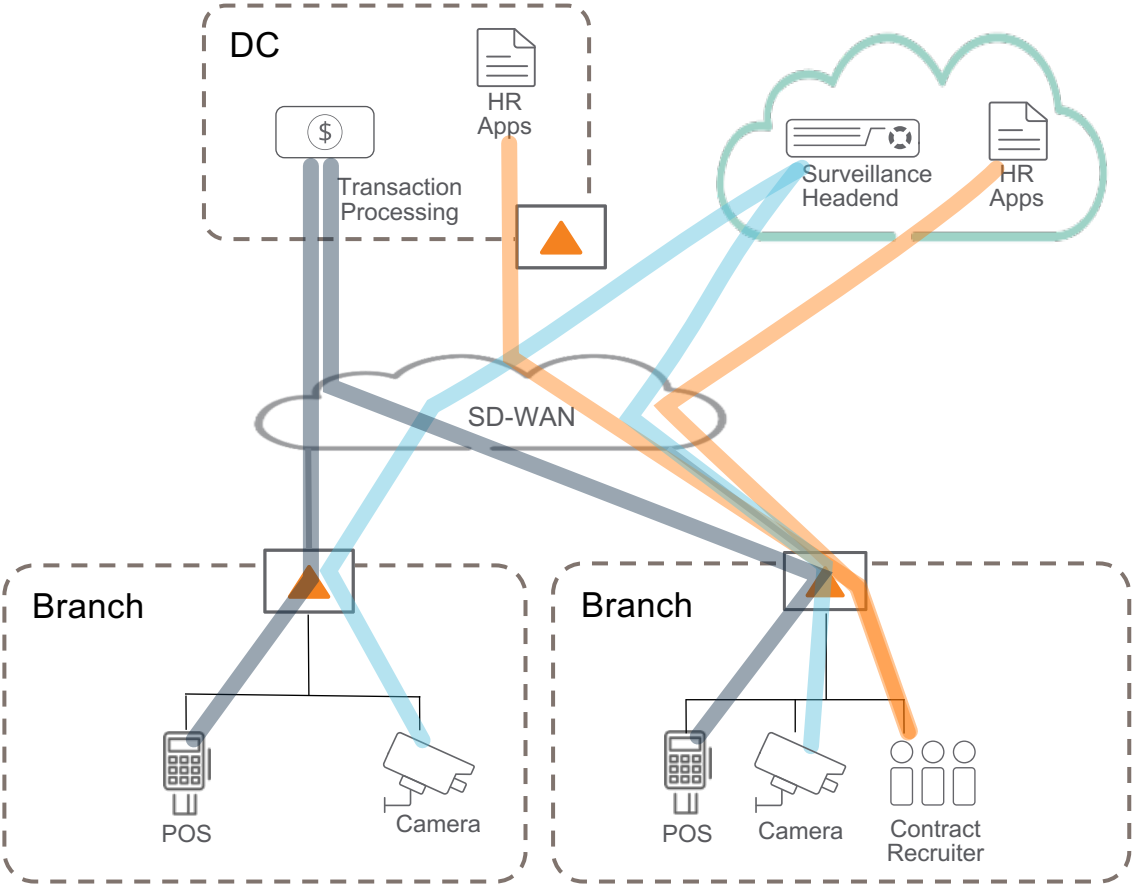
- Threat trending over time
- Overlay with app/user launch and network direction
- Threat source and impact

## Policy-driven enforcement

- Out of box IDS / IPS policies
- User defined whitelisting
- False positive management flow
- Segmentation (Dynamic & VRFs)

# EdgeConnect Zero Trust dynamic segmentation

Users/devices can only communicate with destinations consistent with their role



- Identify users and devices by identity, role and security posture
- Dynamically segment and isolate application traffic based on context
- Business-driven policy example

	Camera	Surveillance Headend	POS Terminal	Transaction Processing	Contract Recruiter	HR Apps
Camera	✗	✓	✗	✗	✗	✗
Surveillance Headend	✓	✓	✗	✗	✗	✗
POS Terminal	✗	✗	✗	✓	✗	✗
Transaction Processing	✗	✗	✓	✓	✗	✗
Contract Recruiter	✗	✗	✗	✗	✗	✓
HR Apps	✗	✗	✗	✗	✓	✓



# Roles and segmentation in ZTA

Identity infused into the SD-WAN fabric in three ways:

1. Retrieve posture and role/username information from the ClearPass Server  
*(display enrichment, no first-packet steering)*
2. RADIUS snooping/proxy  
*(first-packet capable)*
3. VXLAN GPID to Role mapping  
*(first-packet capable)*

## Universal Match Criteria used for:

- QoS Policy
- Firewall Policy
- WAN Optimization (Boost Policy)
- Steering (Zscaler vs. Local Breakout)
- Reporting
- IDS/IPS

The screenshot shows a 'Match Criteria' configuration window. It has a title bar with a close button (X). Below the title bar is a section titled 'Select Match Criteria'. This section contains several rows, each with a checkbox and a text input field:

- Application Group ☐ Type to select
- Application ☐ Type to select
- User Role ☐ Enter Role
- User Name ☐ Enter Source User Name
- User Group ☐ Enter Source Group
- User Device ☐ Enter Source Device
- User MAC ☐ Enter Source MAC

Below these rows is a section titled 'Or Match Using ACL' with a checkbox and a text input field:

- ACL ☐ Type to select

At the bottom of the window is a 'Summary' section with the text 'Match Everything'. In the bottom right corner, there are 'Save' and 'Cancel' buttons.